RICS professional statement, global
Data handling and prevention of cybercrime
1st edition

RICS professional statements

Definition and scope

RICS professional statements set out the requirements of practice for RICS members and for firms that are regulated by RICS. A professional statement is a professional or personal standard for the purposes of RICS *Rules of Conduct*.

Mandatory vs good practice provisions

Sections within professional statements that use the word 'must' set mandatory professional, behavioural, competence and/or technical requirements, from which members must not depart.

Sections within professional statements that use the word 'should' constitute areas of good practice. RICS recognises that there may be exceptional circumstances in which it is appropriate for a member to depart from these provisions – in such situations RICS may require the member to justify their decisions and actions.

Application of these provisions in legal or disciplinary proceedings

In regulatory or disciplinary proceedings, RICS will take account relevant professional statements in deciding whether a member acted professionally, appropriately and with reasonable competence. It is also likely that during any legal proceedings a judge, adjudicator or equivalent will take RICS professional requirements into account.

RICS recognises that there may be legislative requirements or regional, national or international standards that have precedence over an RICS professional statement.

Document status defined

The following table shows the categories of RICS professional content and their definitions.

Publications status

Type of document	Definition
RICS Rules of Conduct for Members and *RICS Rules of Conduct for Firms*	These Rules set out the standards of professional conduct and practice expected of members and firms registered for regulation by RICS.
International standard	High-level standard developed in collaboration with other relevant bodies.
RICS professional statement (PS)	Mandatory requirements for RICS members and regulated firms.
RICS guidance note (GN)	A document that provides users with recommendations or an approach for accepted good practice as followed by competent and conscientious practitioners.
RICS code of practice (CoP)	A document developed in collaboration with other professional bodies and stakeholders that will have the status of a professional statement or guidance note.
RICS jurisdiction guide (JG)	This provides relevant local market information associated with an RICS international standard or RICS professional statement. This will include local legislation, associations and professional bodies as well as any other useful information that will help a user understand the local requirements connected with the standard or statement. This is not guidance or best practice material, but rather information to support adoption and implementation of the standard or statement locally.

Glossary

Cardholder data	Relevant banking card details including name, account number and expiry date.
Client data	Non-public, non-personal data or information pertinent to an independent entity, such as a building or company, that may be used to undertake measurements, valuations or other calculations.
Compliance	Refers to the level of conformance to a given set of standards, legislative, regulatory and other authoritative requirements.
Data	Information collected for reference or analysis.
Data breach	The intentional or unintentional release of personal or client data into an untrusted environment.
Data handling	Any activity that relates to the storage, archiving, processing or deletion of data in a safe and secure manner.
Data handling representative	An individual responsible for ensuring that data is used appropriately and the relevant control measures have been implemented.
Data processing	A subset of data handling that comprises the series of operations carried out on data in order to present, interpret or obtain information.
Data subject	An individual who is the subject of personal data.
Insecure network	Any network containing public or untrusted devices not managed and maintained internally, or by a trusted third party.
Internal network	Any network containing devices managed and maintained by the company or a trusted third party that only directly communicates with other internal networks, secure networks and/or perimeter networks.
Perimeter network	Any network containing devices managed and maintained by the company or a trusted third party that communicates directly with devices on an insecure network, internal/secure network or other perimeter networks.
Personal data	Any information that relates to an identified, or identifiable, living individual.
Penetration testing	An authorised, simulated cyberattack on a computer system, performed to evaluate the security of the system.
Phishing	A fraudulent attempt to obtain sensitive information via email or other electronic communication while disguised as a trustworthy entity.
Principal position	A role in an RICS-regulated firm that falls within the definition of a principal in the *Rules for the Registration of Firms*.
Secure network	Any network that is managed and maintained by a company or individual and contains devices that store, process or transmit data protected by firewalls, intrusion detection systems, antivirus software and, optimally, threat management components.
Sensitive personal data	A special category of personal data, which may include detailed information about an individual including matters such as religion, sexual orientation or genetic data, and when processed may uniquely identify an individual.
Significant data breach	A personal data breach that is deemed important enough to warrant reporting to the relevant authority under local legislation, or a data breach involving client data that is deemed important enough to warrant reporting to RICS.
Subject access request	A request allowing an individual to obtain information about data being held about them, in order to ensure its lawfulness and accuracy. This includes:

	• the personal data an organisation holds on the individual • confirmation it has been processed and • supplementary information (often detailed in an organisation's privacy policy).
System administrator	A person who is responsible for the upkeep, configuration, and reliable operation of computer systems and multi-user computers, such as servers.
Technology infrastructure	The physical and virtual resources that support the flow, storage, processing and analysis of data in its digital form.
User privileges	The rights that define user access to data and functionality on servers and applications.
Virtual Private Network (VPN)	A VPN extends an internal network across an insecure network through the using of internet tunnelling protocols, often employing encryption to secure the data being transmitted.

1 Introduction

The surveying profession has a duty to remain vigilant around the use of data, not only due to the introduction of stricter national laws concerning the correct performance and disclosure of data processing activities, but also because the implications of data loss have never been greater.

With the introduction of data laws such as the EU General Data Protection Regulation (GDPR), many organisations and individuals have become aware of the importance of handling personal data securely. GDPR and other national legislation rarely concern themselves with data defined in other realms, but for the surveying industry this data is central to many tasks. This professional statement defines client data, which is non-public, non-personal data or information relating to buildings or companies that is often used to undertake measurements, valuations or other calculations, and the way it should be handled in order to ensure clients of the industry are protected from data or financial loss and exploitation.

The first line of defence against data loss and cybercrime is through education and best practice, even when the protection of data is a contractual obligation between companies that provide services which involve the use of client data. Market feedback highlighted concerns around the lack of professionalism in understanding and correctly performing data handling procedures.

This professional statement sets out best practice in the handling of both data and the prevention of cybercrime, and provides mandatory obligations that RICS members and regulated firms engaged in this area must comply with.

Principals in RICS-regulated firms must ensure that their firms, and everyone employed in them, comply with this professional statement.

It is important to note that data does not exist only in digital form and may be in the form of printed material, or other tangible storage media such as tapes, written notes or photographs. The scope of this professional statement includes the handling and processing of non-digital data, as well as digital data.

1.1 Effective date

This professional statement (PS) takes effect from xxxx 2019.

2 Mandatory requirements

This professional statement has been developed to raise the standards expected of the modern surveyor in a data-driven world.

1 RICS regulated firms **must** conduct and document an assessment of the risks to personal and client data associated with their work and processes, review this assessment at least annually, and set and document data controls to mitigate the risks they have identified.

2 RICS regulated firms **must** define, maintain and adhere to a data retention policy detailing the length of time for which data is stored.

3 RICS regulated firms **must** ensure that the purpose for which the data is being kept is recorded, including information as to whether the information would be considered personal data, sensitive personal data or client data.

3 RICS regulated firms **must** ensure that a record of data processing activities involving the use of client data is kept, along with any records of documented activities involving personal data and/or sensitive personal data.

4 RICS regulated firms **must** have knowledge of the location of any data and the relevant jurisdictional regulations governing that location. This is particularly relevant for any personal data or client data that is stored offsite or that is replicated in data centres in distant locations.

5 RICS regulated firms **must** take reasonable steps to ensure all suppliers that will process personal data or client data conform to national legislation concerning data handling in both the originating region and the region in which the supplier is located.

6 RICS regulated firms **must** demonstrate the appointment of a person responsible for enquiries and controls pertaining to data handling.

7 RICS members **must** follow controls and protections put in place by an employer.

8 RICS regulated firms **must** use passwords to control access to computers and/or mobile devices used for work purposes.

9 RICS regulated firms **must** ensure the storage of online data and the provision of online services are protected by a firewall at all times.

10 RICS regulated firms **must** use antimalware and antivirus software at all times.

11 RICS regulated firms **must** enforce the use of data encryption when processing sensitive personal data, and must use strong encryption (128-bit or above) and/or security protocols such as SSL/TLS, SSH or IPsec to safeguard sensitive personal data or cardholder data during transmission over insecure networks.

12 RICS regulated firms **must** put controls in place to protect against fraud and cyberattacks when the data involved relates to payment details, by having accounting or work procedures in place requiring authentication of payment details through a second, different, method of contact with the client or supplier.

13 RICS regulated firms **must** ensure that all personal data, sensitive data or client data, however held, is inaccessible to those who should not have access to it at any time. If in written form, it **must** be kept separate and secure, in locked storage, to the satisfaction of the data handling representative or another senior independent person. This policy contributes to the separation of information required by *Conflicts of interest* (1st edition), RICS professional statement, Part 1, section 3.

14 RICS regulated firms **must** create regular data backups.

15 RICS members **must** consider whether they or their employer has appropriate IT security protections in place for the personal data and client data that they handle as part of their work, and if necessary take additional reasonable steps to protect that data.

16 RICS regulated firms **must** ensure that the use of any client data is acceptable through appropriate contractual clauses, or that any such data used in the act of performing a measurement, calculation or valuation is owned or licensed for such use.

17 RICS regulated firms **must** obtain consent to store and process personal data, sensitive personal data and client data through following the correct procedures in all instances.

18 RICS regulated firms **must** be able to demonstrate this consent, and data pertaining to individuals **must** only be held for as long as is necessary (documented in a data retention policy) unless other contractual or legal obligations apply.

19 RICS regulated firms **must** ensure an appropriate record of any necessary consent by the respective data subjects is maintained for data handling and data processing, and that policies relating to personal or private data also apply to any use of client data.

20 RICS regulated firms **must** ensure that appropriate data handling regulators (see appendix A) are notified in the event of a significant data breach within specified timescales, where required by legislation.

21 21 RICS regulated firms **must** consider whether RICS and/or affected data subjects should be notified of a significant data breach, either because it is required by legislation or because of the risks arising from the breach. Where notification is necessary, this **must** be done promptly, and usually within 72 hours of becoming aware of the breach.

22 An RICS regulated firm **must** keep records of any data breach alongside a documented data breach policy. These records **must** include a detailed consideration of whether any notifications were necessary and confirmation of any notifications made, and **must** be made available for subsequent review on request by RICS.

23 In the event of any data breach, RICS members **must** adhere to any legislation and policies set by their employers. They **must** ensure that the relevant data handling representative has been notified and that the breach is reported as soon as is practicable, where this is required by legislation or policies, or the member considers it is necessary.

24 An RICS member **must** report a significant data breach to the appropriate data handling regulator and/or to RICS if the firm in which they work has failed to make a report that the RICS member believes is necessary due to a legislative requirement or the level of risk arising from the data breach.

25 RICS members **must** report concerns about appropriate controls on data handling to senior staff members.

These mandatory requirements represent what is considered to be an acceptable standard of performance for RICS members and regulated firms.

3 Best practice principles

These principles underpin and support the mandatory requirements listed in chapter 2 of this professional statement.

The scope of RICS professional statements encompasses all RICS members, some of whom work within non-regulated firms. It is understood that members are not always able to dictate the controls in place within the firm, but it is expected that members personally show diligence and best practice around the reliability and security of personal and client data.

Where working in collaboration with others, an RICS regulated firm should put binding agreements in place to protect the security and reliability of personal and client data used or shared during the collaboration.

The right to process and handle personal data is often expressed explicitly by data subjects through contractual agreements or 'opt-in' checkboxes on websites. Although this is a common form of consent, and is required to fulfil consensual obligations set out in GDPR legislation, implicit consent may be derived through common interactions with clients.

For example, if a client sends an email to a company in order to understand how a service was delivered, this provides implicit consent to be contacted by the company to which the email was addressed about that service. Similarly, handing over a business card at a meeting demonstrates implicit consent to be contacted about services that could be reasonably considered to pertain to the original context of the meeting.

However, care should be taken when consent is assumed around marketing activities. In these instances, explicit consent should be obtained. When in doubt, speak to the appointed data handling representative, or your regional data handling regulatory body (see appendix A for a list of data handling legislative bodies by country).

3.1 Technology infrastructure

With regard to their technology infrastructure, RICS regulated firms and RICS members in principal positions should:

- review the software and hardware in use and keep it up to date through the installation of patches and firmware upgrades
- maintain an asset register and dispose of assets in a secure manner
- periodically review system logs and access restrictions
- use only company approved equipment on internal networks
- store computers that are not in use in a secure location and ensure the use of security cables to secure PCs to desks where appropriate
- use encrypted email for highly sensitive communication and
- implement two-factor authentication where access to client data and personal data is deemed a significant security risk.

Data logging, the automatic act of writing file and device access records, should be maintained for access to personal data or client data, and used retroactively in the event of a data breach to understand the implications of the breach.

Each instance of a user logging in to applications that store personal data or client data, and each export request, should be logged where it is feasible to do so. The log should be maintained for at least three months. These records may be investigated in the event that a breach is detected to discover which device or user accessed the affected systems. Therefore, it should include details such as the location the access originated from (i.e. the IP address); the time and date of access; and, where applicable, the data requested.

One best practice approach is proactive monitoring, in which alerts are generated upon the detection of abnormal behaviour. This allows system administrators to respond to alerts rather than have to review large log files. It is also important that log event times should be synchronised across all

devices. This ensures that the time logged on each system is accurate and allows for cross-referencing. If files or applications are hosted across multiple servers, established services such as Network Time Protocol (NTP) can be used for time synchronization, and the system administrator should be able to ensure this capability is configured correctly.

User privileges should be reviewed and monitored regularly. The number of privileged accounts (those that have elevated access rights beyond the standard levels) should be minimised.

For RICS regulated firms that support mobile and/or home working, this should be enabled though the use of secure Virtual Private Networks (VPNs) rather than relying on data being stored on user-owned devices.

RICS regulated firms may wish to consider performing internal and external penetration testing, both at regular intervals and after any major system upgrade. It may then form part of best practice procedures to gain further insight into the security of their infrastructure and data systems.

3.2 Data handling

In addition to the mandatory requirements on data handling outlined in chapter 2, RICS regulated firms and RICS members in principal positions should:

- perform regular testing of data recovery procedures
- hold regular data security training sessions
- avoid the use of default passwords and update passwords periodically
- store sensitive personal data in separate parts of the IT infrastructure (either logical or physical), ensuring access control is maintained and
- ensure screen locks are enabled on unattended computers.

RICS members should:

- attend data security training awareness courses where available
  avoid the use of default passwords for any of the systems they have access to, and update their passwords periodically
- make use of data encryption where possible and appropriate and
- follow the data retention policies of the relevant organisation.

Encryption of data is important to ensure that data breaches cannot happen through the loss of IT equipment. Laptops, external hard drives and USB flash drives are especially vulnerable to the theft or accidental loss of the data they contain, and therefore should be encrypted at all times. Encryption usually requires the entry of a password upon device start-up (before any user-associated password request) and ensures that the device is unreadable without the encryption password. This is not the case with standard user account passwords, which simply prevent unauthorised access to user files or services.

Apple Mac computers are encrypted without the need for any action by users, but not all Windows PCs have encryption enabled by default. Encrypting File System (EFS) is a service available on Windows 10 and should be used – as a minimum level of security – to encrypt personal and client data. Another tool available to Windows users is BitLocker, which is a utility that encrypts the entire hard drive.

Data recovery tests should take place at least once a year to ensure that offsite backups are usable, and should often be tested in conjunction with disaster recovery testing, which tests an organisation's resilience when key services are disrupted. The recovery process should be tested using process documents that should be accessible by other methods than through the company network. For example, this can be achieved by ensuring the relevant documents are printed and stored in a secure location, ideally offsite, to ensure they can be accessed in the event that a disaster affects access to the building.

Regular data security training should be delivered to staff at all levels, and cover guidance on data handling and local regulations. Attendance registers for these training sessions should be maintained,

in order to ensure all staff have taken part. Training should encompass issues such as email security and the use of personal data and sensitive data.

3.3 Compliance

RICS regulated firms should:

- maintain policies pertaining to data breaches and malware detection that are reviewed annually, in order to document the processes and procedures that should take effect upon either malware detection or the discovery of a data breach.
- implement secure audit trails to record data access and updates linked to individual user accounts and
- provide contact details for the person responsible for the oversight of data handling, either through a publicly available website or upon request.

An RICS regulated firm's risk register should include risks arising from significant data breaches or malware attacks.

The risk assessment required by RICS regulated firms should consider the amount and nature of personal and client data held; where and how it is held; the processes and technical protections in place to prevent unauthorised access, loss, or events that would adversely affect the reliability of the data; and the likely harm that would be caused by a data breach.

Data handling policies should include contact details for the company's data handling representative, the IT team and any external communications team. These procedures should be referenced, along with the appropriate invocation steps, to alert data centres and offsite backup service providers where required.

Data handling policies should also give guidance on when a breach must be reported to a regulator, and when it should be reported to the affected data subject and/or RICS.

Significant data breaches should be reported to the affected data subject(s) and/or RICS where the RICS regulated firm considers that the breach is likely to result in a high risk of adversely affecting individuals' rights or freedoms, or of damaging the reputation of the profession.

Records kept by an RICS regulated firm of data breaches should also include information about how the breach occurred, and any steps that have been taken by the firm to mitigate the risk of future breaches arising from the same cause or causes.

4 Best practice in common use cases

4.1 USB flash drives

Memory sticks, flash drives and portable hard drives provide convenience at the cost of potential data loss. Not only can these devices be easily misplaced or stolen, they can also store large amounts of data, and are therefore the most common cause of data breaches. Therefore, encryption software should be employed while transferring or storing personal or client data using any external storage device. Many flash drives come with preinstalled software that enables a passcode to be configured; providing file access is not available without this password, such a device can be considered secure.

However, flash drives also provide a route for malware to enter an otherwise clean computer. Avoid using devices whose history is not fully known, as they may have been tampered with. USB drives should be set to prevent them from running automatically when inserted into a computer.

Files that are not immediately recognisable should not be opened, and USB devices of unknown origin should never be inserted into computers that contain, or are connected to any other PC that contains, data that should be protected.

4.2 Physical access

The best PC protection, software, policies and procedures can be rendered worthless if an intruder gains access to the unlocked physical machine. Access by third parties should be recorded to ensure traceability.

Personal and client data should always be protected, and where possible should be kept separate from the rest of the system. If third parties require access to this data, it should be anonymised where possible. If this is not possible, access by authorised third parties should be constantly monitored..

Care should be taken when accessing data outside of the office environment. Do not connect to public wireless hotspots with devices that contain or access private data, and be aware of the visibility of device screens in public locations. Data loss is not always in digital form – it is possible for data to be leaked through information that is visible to third parties observing the screen of a device.

4.3 Mobile devices

While some organisations have a ‘bring your own device’ policy at work, most recognise the difficulty of managing such a policy. If an employee must access data on their own device, it is important that this data is only stored temporarily on the device, or that the organisation’s IT team has the ability to remotely delete it. Furthermore, such devices must be secure and access to the organisation’s systems from them should be logged. It is important that these devices are securely wiped in the event of their sale or loss, or when the employee leaves the company.

4.4 Cloud storage

Cloud-based mass storage utilities such as OneDrive, DropBox and Google Drive are often used as a convenient option to centralise and share data across an organisation. It is important to understand the exact nature of their storage facility, such as where the data is stored, under what terms the data is made available and how data access is administered.

With data that is stored, digitally or otherwise, in a location that is not on the firm’s premises and/or hardware, it is important to ensure that it is still only kept for as long as is required. Companies can minimise the scope and magnitude of potential data breaches by minimising the amount of data that is held and regularly reviewing stored data to assess whether it can be deleted. In order to do this in an efficient manner, either a content management system (CMS) should be employed or a file structure that simplifies this task should be utilised (for example by naming folders by clients and including sub-directories that reference the date by which the data should be removed).

4.5 Email

Many filetypes that are often considered safe to send as email attachments, such as PDFs, can contain viruses or malware. Therefore, it is important to treat such files with care, and avoid executing unknown files when opening attachments that are sent from unknown contacts.

Emails should be organised logically in subfolders, in order to simplify the process of reviewing and deleting them when no longer required by the company's data retention policy, and only stored for as long as the company's data retention policy dictates. For most organisations, 6 years should be sufficient.

Members should avoid sending private data by email. If this is required, public key cryptography or transport encryption provided by technology such as STARTTLS should be used.

To reduce the likelihood of successful email phishing scams against employees, organisations should consider running email safety awareness courses.

4.6 Passwords

Secure passwords are those that are not easy to guess, either heuristically or through brute force. A password may be discovered by an intruder through brute force by testing thousands of 'known' passwords ('password123', 'qwertyuiop', 's3cretpa55', etc.), or through heuristic methods such as combinations of birthdays and pet names.

In practice, this means using passwords that are more than seven characters in length and include both upper and lower case letters, numbers and symbols.

It is important to use different passwords for each different site or utility that requires one, so that if one account is compromised, other accounts are not affected. To help manage multiple passwords, a password management utility is recommended over other forms of password documentation. Where passwords are required for a shared service, such as the administration of a centralised server, a physical password vault can be utilised.

Appendix A Data handling regulatory bodies by country

Austria	Austrian Data Protection Authority (DSB)
Belgium	Commission for the Protection of Privacy (CPP)
Bulgaria	Commission for Personal Data Protection (CPDP)
Croatia	Personal Data Protection Agency (AZOP)
Czech Republic	Office for Personal Data Protection (UOOU)
Denmark	Danish Data Protection Agency (Datatilsynet)
Estonia	Estonian Data Protection Inspectorate (DPI)
Finland	Data Protection Ombudsman (Tietosuojavaltuutettu)
France	Commission nationale de l'informatique et des libertés (CNIL)
Germany	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)
Greece	The Hellenic Data Protection Authority (HDPA)
Hungary	National Privacy and Data Protection Authority (NAIH)
Ireland	Data Protection Commissioner (DPC)
Italy	The Italian Data Protection Authority (Garante)
Japan	Personal Information Protection Commission (PPC)
Latvia	Data State Inspectorate (DVI)
Lithuania	The State Data Protection Inspectorate (VDAI)
Luxembourg	National Commission for Data Protection (CNDP)
Malta	Office of the Information and Data Protection Commissioner
Netherlands	Personal Data Authority (PDA)
Poland	General Inspector for the Protection of Personal Data (GIODO)
Portugal	The National Commission for Data Protection (CNDP)
Republic of Cyprus	Office of the Commissioner for Personal Data Protection
Romania	The National Supervisory Authority for Personal Data Processing
Slovakia	Office for Personal Data Protection (PDP)
Slovenia	The Information Commissioner
Spain	Agencia Española de Protección de Datos (AEPD)
Sweden	The Swedish Data Protection Authority (Dataprotektionen)
UK	The Information Commissioner's Office (ICO)
United States	U.S. Federal Trade Commission (FTC), in conjunction with each individual State.

Appendix B Relevant organisational documents

Organisations should maintain the following documents, which detail the relevant procedures and policies:

Risk register	Details key risks, risk owners, mitigating steps and both severity and possibility. Severity measures how critical the impact of a potential risk may be, and possibility relates to the likelihood of the risk occurring. For example, a server-room fire may be classed as 'high severity' and 'low possibility', since the result may be catastrophic, but it is unlikely to occur.
Data retention policy	Documents how long data should be stored and backed up, both onsite and offsite. Describes

	who is responsible for data removal and how data is identified as being 'out of date.
Data breach procedure	Describes the process to follow when a breach is identified or reported to the organisation. Should include contact details of the associated regulatory bodies, timescales and stakeholders who are responsible for carrying out the plan.
Data compliance statement	Describes how the organisation is compliant with data protection laws. This document should also include details of how users can ask for their data to be removed, and the process for subject-information requests, should the company support this.
Data processing details	Documents what personal data and client data are held and the reason for processing that data.
Roles and responsibilities of the data handling representative	Document detailing the roles and responsibilities of the data handling representative.
Data backup and recovery process	Documents which servers, applications and physical files are backed up, how often and the process by which the files are archived. Contact details of the relevant offsite recovery centres, and the process by which the data can be recovered and tested, should also be stored.
Business continuity document	References the data backup and recovery processes, but should also include details about physical infrastructure such as telephony, PC and email access instructions in the event of a major disaster that renders either the building, IT infrastructure or key personnel unavailable.